Decisive Use of IO

By Robert K. Lyman, Lieutenant Colonel, USAF

Editorial Abstract: Lt Col Lyman examines how US military professionals continue to question whether information operations are truly a decisive form of tactical warfare. He describes how this is possible, if it allows a marked advantage over an adversary, or is used in the offensive. He analyzes operational examples including PSYOP and MILDEC in Desert Storm, and EW in the Battle of Britain, to demonstrate IO's decisiveness.

Winner: The Excellence in Joint Command, Control, Communications, Computers and Intelligence (JC4I) / Information Operations (IO) Writing Award, United States Army Command and General Staff College, 2007.

Are Information Operations a Decisive Form of Tactical Warfare?

As the information operations capabilities of the United States military continue to mature some national security professionals continue to question whether information operations (IO) are truly a decisive form of tactical warfare, and whether IO can do more than shape the battlefield for more traditional capabilities. In order to answer these questions fully it is necessary to clarify exactly what IO is, define the tactical level of war versus the other levels, and explore what decisive means. Buried in these definitions, and in the ways we describe their application, are clues to the answer. Given clear doctrinal definitions of these terms, and a brief exploration of IO related doctrine, just a few historical examples, and a few hypothetical ones, will clearly show that IO can be decisive.

What is IO?

In Joint doctrine, "information operations (IO) are described as the integrated employment of electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC), in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own." IO supporting capabilities include information assurance (IA), physical security, physical attack, counterintelligence, and combat camera. Capabilities related to IO include public affairs (PA), civil-military operations (CMO), and defense support to public diplomacy.

Which level of war? (Defense Link)

Tactical Level of War

US doctrine recognizes three levels of war. The strategic level, the highest of the three, is the level at which a nation determines national, or multinational, security objectives and uses national resources to achieve them. The next lower lever, operational, is the level "at which campaigns and major operations are planned, conducted and sustained to achieve strategic objectives within theaters." The tactical level is the "level of war at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. Activities at this level focus on the ordered arrangement and maneuver of combat elements in relation to each other and to the enemy to achieve combat objectives". US military doctrine states that "IO capabilities can produce effects and achieve objectives at all levels of war and across the range of military operations." For IO to be decisive at the tactical level it must the capability used by a tactical unit to achieve combat objectives in a battle or engagement.

What is Decisive?

Planners at the strategic and operational levels focus on the enemy center of gravity (COG). Since the question at hand deals with the tactical level it is important to note that "generally, there is no COG at the tactical level but decisive points instead." Again it is helpful to look at a doctrinal definition. The definition of decisive point is "a geographic place, specific key event, critical factor, or function that, when acted upon, allows commanders to gain a marked advantage over an adversary or contribute materially to achieving success." Thus use of an IO capability must allow a commander to gain a marked advantage over an adversary to be decisive at the tactical level. It is important to note that US military doctrine also highlights that "it is the offense that is normally decisive in combat." Therefore the IO capability must be used in the offense to be decisive.

Unfortunately, the word "decisive" is only used once, in a glossary definition, in the entire IO joint publication. So given our definitions, which of the IO core capabilities could be decisive? As a form of fires it is likely that EW could be decisive. The Computer Network

Attack aspect of CNO could be decisive. PSYOP could be decisive if it is effective at influencing the behavior of foreign actors and giving a commander a marked advantage. MILDEC could be decisive if it effectively causes the adversary to take an action (or inaction) that is decisive in accomplishment of the friendly mission. Tactical MILDEC "serves to exploit the immediate tactical situation," thus it could give a commander a marked advantage.

A further look at doctrine finds a number of references to IO and decisiveness. Joint Publication (JP) 3-0, *Joint Operations*, alone gives two examples. "Given the appropriate circumstances, any element of military power can be dominant—and even decisive—in certain aspects of an operation or phase of a campaign, and each force can support or be supported by other forces." As an element of military power, IO could be decisive. "Against unconventional enemies, decisive operations are characterized by dominating and controlling the operational environment through a combination of conventional/ unconventional, information, and stability operations." Again, IO is noted as an element of decisiveness.

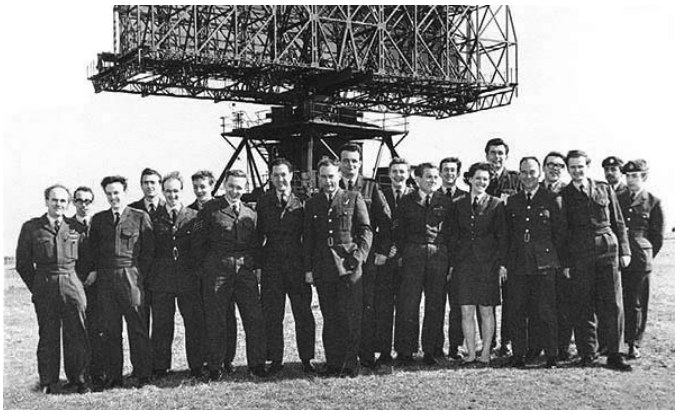
The Army's new counterinsurgency manual also highlights some of the decisive aspects of IO. The manual notes that "IO must be aggressively employed" to "favorably influence perceptions of host nation legitimacy". Joint doctrine highlights legitimacy as a principle of war, and states, "legitimacy is frequently a decisive element." The counterinsurgency manual also notes when discussing logical lines of operations (LLO) that "the IO LLO may often be the decisive LLO," and that "the IO LLO may be the most important one." Clearly US military doctrine has embraced the idea that IO can be decisive.

Doctrinal definitions lead us toward an understanding that IO can be decisive at the tactical level if it meets three general criteria. First, an IO capability must be used by a tactical unit to achieve combat objectives in a battle or engagement. Second, the use of the IO capability must allow a commander to gain a marked advantage over an adversary. Third, the IO capability must be used in the offensive to be decisive. It would seem that further focus on the five core capabilities noted in the IO definition is needed, specifically those that could be used offensively. Doctrinal definitions of each, with appropriate operational examples, follow.

Decisive Examples of IO Core Capabilities

EW is "military action involving the use of electromagnetic and directed energy to control the electromagnetic (EM) spectrum or to attack the enemy. Electronic warfare consists of three divisions: electronic attack, electronic protection, and electronic warfare support." Electronic attack would be the offensive form and "EA involves the use of EM energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires." Specifically EA includes EM jamming, EM deception, directed energy, antiradiation missiles, and expendables such as flares and active decoys.

One possible example of decisive use of EW was the use of radar by the Royal Air Force (RAF) in Battle of Britain in 1940. Radar was mainly used for threat warning, which falls under EW support and not EA , but it did give the RAF a marked advantage over the Luftwaffe. The British established a number of coastal radar stations that were able to pick up incoming German warplanes. They paired the radar stations with a communications network centrally linked back to their air headquarters, and added an Observer Corps who augmented the radar with visual scans and timely reports. This centrally linked command and control system made the British air defense system much more agile in responding to German attack, particularly at vectoring RAF fighters against the invading bombers. The central RAF headquarters would vector individual RAF combat air patrols against Luftwaffe bombers, allowing them to find, approach and engage the Germans to their advantage and before the Germans knew exactly where they were, in much the same way that modern Airborne Warning and Control System aircraft and Joint Surveillance Target Attack Radar System aircraft direct attacks on air and ground targets. While the threat warning portion may look like an electronic protection or EW support capability, when paired with one of the IO supporting capabilities, physical attack in this example, it seems to meet the criteria to be decisive. The capability was used by tactical fighter aircraft in an engagement, it gave them a marked advantage, and it was used in an offensive capacity to attack incoming aircraft. Hypothetically it is also easy to conclude that directed energy or antiradiation missiles could be decisive at the tactical level as well, in taking out a specific target or emitter in a specific engagement.



Early decisive IO warriors: a Royal Air Force Electronic Warfare team. (Subterranea Brittanica.org)

CNO is "comprised of computer network attack, computer network defense, and related computer network exploitation enabling operations." Specifically computer network attack is "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves." Computer network defense is "actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks." Computer network exploitation is "enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks."

In the months leading up to Operation Desert Storm in 1990-1991 the US and United Kingdom intelligence services undertook an operation to disrupt Iraqi C2, and deny or degrade its use when coalition forces attacked. This computer network attack never came to fruition since the C2 network was destroyed by airpower just before ground forces pushed north, but it is feasible that it could have had the same effect had it been given time to be fully implemented.

While the US military has focused their use of technology on the modern battlefield other groups around the world have watched the advance of technology and have found other innovative ways to use it to their advantage. There is evidence that Al Qaeda and other terrorist organizations have used the commercial Internet to plan terrorist attacks, to raise significant amounts of money, share intelligence, and to command and control world-wide terrorist cells. Additionally, the Internet has allowed Al Qaeda to exploit world-wide mass media by putting out false messages, highlight US and coalition mistakes, and publicize their ideology, all with minimal interruption from their enemies. Insurgent groups in Iraq and elsewhere have also used the Internet for the same

Decisive IO warrior in action. (Defense Link)

purposes. Chechens used the Internet very effectively in their fight against the Russians in 1999. They posted videos of Russian defeats, unfiltered opinions on the Chechen cause, and calls for monetary support, even publicizing bank accounts around the world to send money to. Successful efforts to thwart terrorist or insurgent use of the Internet have been limited at best. This is an area where the weaker combatant is using technology asymmetrically to their advantage, and there is yet to be a successful campaign to combat it.

None of these actions necessarily fall into the computer network attack definition, but if these groups had the capability to launch a cyberattack against their nation-state enemy they clearly would. If insurgents in Chechnya or Iraq were able to attack the power supply system, telecommunications system, or transportation network through a computer network attack and were successful in disrupting or degrading them during a key timeframe, particularly if the timing was linked to other insurgent or terrorist operations, then that could be considered decisive. When researching critical US infrastructures and the threat to them, the interagency Critical Infrastructure Working Group identified telecommunications as one of eight critical infrastructures which were deemed "so vital that their incapacity or destruction would have a debilitating impact on a regional or national level." While an attack on that scale would likely be viewed as strategic or operational, its effects would be felt at the tactical level and could be paired with other IO supporting capabilities for a decisive effect. Such attacks could also be limited to a tactical objective, such as the power or telecommunications system in only one city or neighborhood for example.

PSYOP is "planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives." PSYOP leaflets dropped on Iraqi forces in the weeks leading up to operation Desert Storm in 1990-1991 led to many thousands of Iraqi soldiers surrendering without a shot. Again, the PSYOP was paired with physical attack and other IO supporting capabilities, but to the coalition battalions that planned to attack the well fortified Iraqi positions in the opening days of the war the effort must have seemed decisive. Another recent example would be Somali warlord Mohammed Farah Aideed and his use of propaganda against his own people to shape their view of United Nations forces. Through the use of both the international media and his local radio broadcasts he effectively manipulated Somali views, and eventually their behavior toward UN forces in Mogadishu.

"MILDEC is defined as those actions executed to deliberately mislead adversary decision makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission." One very successful modern example of MILDEC would be the effort by coalition forces in 1991 to convince the Iraqis that they would be facing an amphibious attack, while really planning the main effort to be the "left hook" operation in the

western desert. This effort forced the Iraqis to mass forces toward the coast leaving them vulnerable. While the MILDEC effort can be argued to be an operational level effort, again the effects were felt down to the tactical level where coalition forces were attacking the Iraqi flank. Perhaps a more tactical level example, although a mythical one, would be the use of the Trojan Horse by the Greeks during the Trojan War. In the ancient story the Greeks deceived the Trojans into bringing the great wooden horse into their city, which unknown to the Trojans hid a contingent of Greek warriors who snuck out and defeated the unprepared Trojans. This decisive deception was used in a battle, gave the Greeks a marked advantage, and was used offensively.

OPSEC "is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information." In short, it "is a methodology that denies critical information to an adversary." Given that definition and that OPSEC is a defensive capability, it would not be decisive.

Conclusion

General Glen Otis, former commander of US Army Training and Doctrine Command, noted after Operation Desert Storm stated that "the combatant that wins the information campaign prevails.…information is the key to modern warfare—strategically, operationally, tactically, and technically." Current US military doctrine supports that view with its many references to IO as a decisive element. Using those references we find that IO can be decisive if an IO capability is be used by a tactical unit to achieve combat objectives in a battle or engagement, if it allows a commander to gain a marked advantage over an adversary, and if it is used in the offensive. A number of recent operational examples demonstrate IO's decisiveness, including the use of PSYOP and MILDEC in Desert Storm and EW in the Battle of Britain. The partially hypothetical example of CNA in the months leading up to Desert Storm shows how CNA could have been decisive had the operation been given time to mature. The rise of global media outlets including the press, television and radio, are all prolific arrows in the IO quiver. Their effective use in the contemporary operating environment make their decisive use essential to victory at not just the tactical level.